CS240A Proposal: Parallelizing Elliptic Curve Cryptography

Qin ZHOU
fatestudio@gmail.com

Liang XIA
liangxia2006@gmail.com

February 6, 2013

1 Introduction

Elliptic Curve Cryptography (ECC) is a public-key technology that offers performance advantages at higher security levels. It includes an elliptic curve version of the Diffie-Hellman key exchange protocol [3] and elliptic curve versions of the ElGamal Signature Algorithm [4]. The adoption of ECC has been slower than had been anticipated, perhaps due to the lack of freely available normative documents and uncertainty over intellectual property rights. [2]

Elliptic Curve Cryptography can be parallelized in several ways:

First we can parallelize the computation of $2P$ in Elliptic Curve, which means parallelizing the computation of equation:

$$x_3 \equiv m^2 - 2x_1 \ (mod\ p) \tag{1}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \ (mod\ p) \tag{2}$$

$$m \equiv \frac{3x_1^2 + A}{2y_1} \ (mod\ p) \tag{3}$$

Second we can parallelize several attacks towards ECC. For example, Pollard's λ method can be parallized by using several different random starting points [1]. There are several other existing parallel attacks, and we can also develop our new attacking methods.

2 Schedule

1. Read some materials;
2. Implement an Elliptic Curve Cryptography algorithm (basic ECC components, or a complete ECDHE) on Triton.
3. Try to use OpenMP, MPI, and pthread to efficiently parallelize the ECC algorithm ;
4. Evaluate the performance data, such as MFLOPS, parallel time, and speedup compared to the original ECC implementation.
5. Implement several parallized attacks towards ECC on Triton.

References

[1] L. C. Washington, "Elliptic Curves Number Theory and Cryptography", Second Edition, 2008

[2] D. McGrew, K. Igoe and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC6090

[3] Diffie, W. and M. Hellman, "New Directions in Cryptography", IEEE Transactions in Information Theory IT-22, pp. 644-654, 1976.

[4] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. 30, No. 4, pp. 469-472, 1985.